Sortie de la version 9.7 de BIND : DNSSEC enfin pour les humains ?

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 18 février 2010

https://www.bortzmeyer.org/bind-9-7.html

Le 16 février, l'ISC a annoncé la disponibilité de la version 9.7 de BIND dont le slogan commercial est « "*DNSSEC for humans*" ». On retrouve ce slogan sur le joli T-shirt offert à ceux qui ont participé au développement, et qui montre l'homme de Vitruve sur fond de clés cryptographiques. (On peut voir ce T-shirt sur la vidéo de mon exposé DNSSEC à JRES 2009 <https://2009.jres.org/planning_files/summary/html/5.htm>.)

DNSSEC a été traditionnellement un cauchemar de configuration et, disons le tout de suite, la version 9.7 ne résoudra pas complètement le problème. Mais elle apporte des améliorations sensibles et on peut donc penser qu'il n'y aura pas de déploiement significatif de DNSSEC avant que la version 9.7 n'aie atteint un grand nombre de sites. Quelles sont les nouveautés de cette version ?

- Gestion du RFC 5011 [1] qui permet à un résolveur de suivre automatiquement les clés successives d'un domaine, sans reconfiguration.
- Configuration simplifié de DLV (RFC 5074) : en mettant `dnssec-lookaside auto`, BIND utilise automatiquement le registre DLV de l'ISC <https://www.isc.org/solutions/dlv> (la clé publique est livrée avec BIND). Tant que la chaîne DNSSEC n'est pas complète, de la racine jusqu'à `example.com`, DLV restera indispensable.
- Amélioration de la configuration lorsque la zone est mise à jour par "*dynamic update*" (RFC 2136) mais ne m'en demandez pas plus, je n'ai pas encore testé.
- Mesures contre les attaques par changement DNS <https://www.bortzmeyer.org/dns-rebinding-pinnin
  html>.
- La bibliothèque DNS est désormais indépendante de BIND (enfin !) et peut donc facilement être utilisée par des applications en C et elle inclut des améliorations pour DNSSEC comme un `getaddrinfo()` validant (nouveau code d'erreur non-standard `EAI_INSECUREDATA`). Cela se configure dans le nouveau et expérimental fichier de configuration `/etc/dns.conf`.

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc5011.txt`

— Nouveaux outils PKCS#11 (mais configurer BIND pour PKCS#11 reste toujours aussi difficile et dépend d'un OpenSSL patché).
— Intégration de la famille SHA-2 suivant le RFC 5702.
— Et beaucoup d'autres (voir la liste complète <https://www.isc.org/software/bind/new-features/9.7>).

BIND 9.7 n'atteindra pas tous les systèmes immédiatement. Beaucoup d'administrateurs système (et à juste titre) n'utilisent pas de version ".0" en production et beaucoup d'autres n'utilisent que les paquetages fournis par leur système d'exploitation (et à juste titre). Notons toutefois que, pour DNSSEC, il y a de bonnes raisons d'accélerer la migration. Par exemple, la validation de la racine nécessitera BIND 9.7 (ou le 9.6, à partir de 9.6.2) car la racine utilise SHA-2 <https://www.bortzmeyer.org/signature-racine.html>.

Et, bien sûr, BIND n'est pas le seul logiciel libre sérieux pour faire un serveur DNS, je recommande également Unbound <https://www.bortzmeyer.org/unbound.html> pour un serveur récursif et nsd pour un serveur faisant autorité.